

eHealth Ontario Privacy and Data Protection Policy

Document Identifier: 00998

Version: 4

Contents

1	Purpose	1
2	Scope and Application	1
3	Context	2
3.1	Protecting Privacy is Central to eHealth Ontario's Mandate	2
3.2	Agency Privacy Requirements.....	2
3.3	Fostering a Culture of Privacy Protection.....	2
4	Policy	3
4.1	Guiding Principles	3
4.2	Policy Requirements	4
	Accountability.....	4
	Privacy Protection Program.....	4
	eHealth Ontario Policies and Practices	5
	Privacy Training and Awareness.....	6
	Working with Third Party Providers	7
	Protecting PI/PHI	8
	Openness	8
	Monitoring Compliance and Performance	8
	Complaints and Inquiries.....	9
	Consequences.....	9
5	Responsibilities:	10
5.1	Board of Directors	10
5.2	President and CEO	10
5.3	Chief Privacy Officer.....	10
5.4	Privacy Office.....	10
5.5	eHealth Ontario Personnel	10
6	Glossary	10
7	Subordinate Policies	12
8	Contact Information	12
9	Interpretation	13

Document Control

The electronic version of this document is recognized as the only valid version

Document Location:	http://www.ehealthontario.on.ca/privacy
Review Frequency:	Annually, or more often at the Chief Privacy Officer's discretion
Document Prime*	Anne Motwani Senior Privacy Analyst

*Enquiries relating to this document should be referred to the responsible Document Prime.

Approval History

Approver(s)	Approved Date
eHealth Ontario Board of Directors	2011-10-13
Chief Executive Officer	2011-10-13
Director, Privacy	2011-10-13
Privacy Leadership Group	2011-09-19

Revision History

Version No.	Version Date	Summary of Change	Changed By
4	2011-10-05	Revisions as per General Counsel	Jane Dargie
3.1	2011-08-31	Revision as per Chief Privacy Officer	Jane Dargie
3	2009-08-12	Revision as per Chief Privacy and Security Officer	Patrick Lo
2	2008-09-26	Revision as per VP, Privacy and Security. Final Revisions completed	Angelique Hamilton
1	2007-09-28	Final draft	Sharan Dosanjh

1 Purpose/Objective

The *eHealth Ontario Privacy and Data Protection Policy*:

- supports decision-making at eHealth Ontario ('eHealth Ontario' or 'the Agency') by establishing guiding principles for how the Agency will protect privacy, and the confidentiality of personal information (PI) and personal health information (PHI);
- establishes policies about how the Agency manages privacy protection in order to enable eHealth Ontario to achieve privacy compliance and a culture of privacy protection and apply 'Privacy by Design';¹ and
- identifies core privacy responsibilities for eHealth Ontario personnel to foster co-ordination among eHealth Ontario divisions and teams in protecting privacy.

2 Scope and Application

This Policy applies to eHealth Ontario's personnel (permanent employees and temporary staff). It applies to:

- Personal Information (PI) protected by the *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F. 31 (FIPPA);
- Personal Health Information (PHI) protected by the *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3 (PHIPA); and
- Any other information that the Chief Privacy Officer (CPO) determines that the Agency shall treat as PI/PHI.

eHealth Ontario maintains a comprehensive set of privacy and data protection policies that are subordinate and complementary to the *eHealth Ontario Privacy and Data Protection Policy*. The subordinate policies, listed in section 7, define privacy roles, responsibilities, accountabilities and requirements relevant to a given context (e.g. for the management of PHI and for PI) and may apply not only to eHealth Ontario but also to parties such as health information custodians and third party service providers.

¹ 'Privacy by Design' is a concept developed by the Information & Privacy Commissioner/ Ontario, Dr Ann Cavoukian which advances the view that privacy assurance must be an organization's default mode of operation; compliance with regulatory frameworks alone is insufficient to protect privacy.

3 Context

The Context section explains why protecting privacy is critical at eHealth Ontario and introduces the sources for the Agency's privacy requirements.

3.1 Protecting Privacy is Central to eHealth Ontario's Mandate

Protecting privacy is not only an obligation for the Agency- it's also part of its mandate. Along with providing eHealth Services and support for the effective and efficient planning, management and delivery of health care in Ontario, and developing eHealth Services strategy and operational policy, the Agency is to: 'protect the privacy of individuals whose personal information or personal health information is collected, transmitted, stored or exchanged by and through the Agency, in accordance with the *Freedom of Information and Protection of Privacy Act*, the *Personal Health Information Protection Act, 2004* and any other applicable law.'²

3.2 Agency Privacy Requirements

The Agency's privacy requirements derive from many sources including:

- Laws, rules, orders, regulations and by-laws, particularly its Enabling Regulation, PHIPA, FIPPA and orders made by the Information and Privacy Commissioner/ Ontario
- The Agency's Memorandum of Understanding with the Minister
- Government of Ontario Directives that apply to eHealth Ontario³
- Agency policies
- Agreements
- Industry best practices
- Stakeholder expectations

The regulatory requirements that apply to any given Agency activity depend on the facts and circumstances involved.

eHealth Ontario's subordinate privacy policies and procedures explain the regulatory requirements in detail.

3.3 Fostering a Culture of Privacy Protection

The Agency believes that protecting privacy effectively involves not only complying with applicable privacy requirements but also having a strong culture of privacy protection.

² Ontario Regulation 43/02, R.S.O. 1990, c. D. 10, as amended from time to time, s3.3

³ The Agency's Memorandum of Understanding with the Minister requires eHealth Ontario to comply with Government of Ontario Directives that apply to eHealth Ontario. The person with authority to make a Directive binding on the Agency is also the person who can exempt the Agency from having to apply aspects of the Directive.

This Policy mandates the Agency's Privacy Protection Program. The Privacy Protection Program comprises comprehensive safeguards for PI/PHI and programs, practices, processes, tools and techniques to protect privacy proactively. eHealth Ontario establishes a culture of privacy protection by maintaining and continuously improving its Privacy Protection Program.

4 Policy

The Agency has established Guiding Principles for its approach to protecting privacy. Section 4 articulates the Guiding Principles which also serve as an interpretative tool for the policies that follow in section 4.2.

4.1 Guiding Principles

1. By proactively protecting privacy and PI/PHI, and fostering a culture of privacy protection, eHealth Ontario:
 - demonstrates respect for individuals' privacy rights and for its stakeholders;
 - reduces privacy, operational and other risks for the Agency and for its stakeholders, particularly the public; and
 - builds confidence in the Agency.
2. Protecting PI/PHI in accordance with the Agency's privacy requirements is a core eHealth Ontario business practice. The Agency's privacy requirements derive not only from legal requirements but also from Agency policies, industry best practices and individuals' privacy preferences.
3. The Agency proactively embeds privacy protections into the design and operation of its programs, services, systems, and processes. Privacy protections shall seek to prevent privacy invasive events from occurring and shall safeguard PI/PHI throughout its lifecycle.
4. eHealth Ontario personnel all play a role in protecting privacy and PI/PHI, working under the leadership of the Chief Privacy Officer (CPO). eHealth Ontario managers, including the CPO, are responsible for making sure that eHealth Ontario manages privacy protection consistently and in a co-ordinated manner.
5. The Agency employs a risk-based approach to protecting privacy. Risk management practices provide the opportunity to establish the optimum level of oversight, control and discipline to enable the Agency to manage risk in changing environments and help provide the proper level of assessment that business objectives and strategies, including privacy protection, are being met.
6. The Agency will continuously improve its Privacy Protection Program. It will seek opportunities to do so by learning from its stakeholders' experience and results, and by encouraging feedback and suggestions, particularly from personnel.

4.2 Policy Requirements

Accountability

1. The Agency's Board of Directors oversees the protection of privacy at eHealth Ontario.
2. The President and Chief Executive Officer (CEO) is responsible for managing privacy protection at the Agency, including ensuring that eHealth Ontario complies with applicable privacy requirements and fostering a culture of privacy protection.
3. The CEO delegates responsibility to the Chief Privacy Officer (CPO) to:
 - lead the design and operation of the Agency's Privacy Protection Program, including privacy-related governance bodies;
 - provide advice, support and direction to personnel about privacy matters applicable to their areas of responsibility; and
 - monitor and report on privacy protection at eHealth Ontario.
4. eHealth Ontario managers are responsible for achieving and demonstrating compliance with privacy requirements applicable to their areas of responsibility.
5. eHealth Ontario shall provide its personnel and third party providers with formal direction on their accountabilities, roles and responsibilities for protecting privacy. Means of providing such direction may include: training and awareness programs, agreements and written policies and procedures and job descriptions.

Privacy Protection Program

6. The Agency shall maintain a Privacy Protection Program that comprises comprehensive and aligned safeguards for PI/PHI, and programs, practices, processes, tools and techniques that enable it to:
 - protect individuals' privacy and the confidentiality of their PI/PHI proactively and respect their privacy preferences; and
 - comply with its privacy requirements, particularly those derived from its Enabling Regulation, from PHIPA and FIPPA and the Regulations made under those Acts, and from its policies.
7. The Privacy Protection Program shall include processes, practices and tools and techniques to:

- build privacy and security protection into the design and operation of the Agency's programs, operations and services, including business practices, systems and physical design and infrastructure;
 - safeguard PI/PHI throughout its lifecycle;
 - achieve, monitor, assess and enforce privacy compliance;
 - identify and manage privacy risks proactively;
 - train personnel about protecting privacy;
 - develop and implement privacy policies, practices and standards;
 - provide privacy and security assurance services such as Privacy Impact Assessments (PIAs) and Threat and Risk Assessments (TRAs);
 - manage, investigate and respond to privacy- and security- related incidents, breaches, complaints and inquiries; and
 - engage internal and external stakeholders about privacy matters.
8. The CPO shall lead the design, implementation and operation of the Privacy Protection Program, working collaboratively with personnel.
 9. eHealth Ontario managers shall design, implement and operate aspects of the Privacy Protection Program applicable to their areas of responsibility, working collaboratively and proactively with the CPO.
 10. eHealth managers shall ensure that privacy risks related to their areas of responsibility are identified, monitored, managed and subject to mitigation. The CPO shall provide tools and methods to achieve that objective, aligned with the Agency's overall risk management approach.
 11. Personnel shall seek to design privacy-protective features, including privacy defaults, into Agency products, services and operations.
 12. The Agency shall conduct privacy and security assessments to accompany any proposals for new initiatives or changes to existing initiatives that may affect individuals' privacy.
 13. At the CPO's direction, eHealth Ontario may extend privacy protections to information that is not subject to privacy and data protection laws, regulations or similar requirements.

eHealth Ontario Policies and Practices

14. eHealth Ontario's policies and practices shall:
 - protect privacy and the confidentiality of PI/PHI while achieving the Agency's other business interests and objectives (e.g. effectively facilitating the delivery of services and programs and realizing value for money); and

- comply with all applicable privacy requirements, in particular the Guiding Principles and Policy Requirements articulated in the Privacy and Data Protection Policy.

15. The CPO shall:

- advise eHealth Ontario managers about the privacy implications of, and requirements for, policies and practices in their areas of responsibility;
- provide advice and support to the Shareholder Relations and Business Planning Department during Agency strategic Policy development initiatives; and
- establish and maintain written policies and practices that direct the design and management of the Agency's Privacy Protection Program.

16. eHealth Ontario managers shall:

- confirm that policies and practices applicable to their areas of responsibility comply with the Privacy and Data Protection Policy and any applicable subordinate privacy policies;
- seek advice from the CPO about the privacy implications and requirements for their policies and practices, particularly at the design stage and when making significant changes; and
- establish, maintain and ensure compliance with written policies and practices that protect individuals' privacy and the confidentiality of PI/PHI applicable to their areas of responsibility.

17. The CPO and Chief Security Officer (CSO) shall ensure that the Agency's policies and practices that protect individuals' privacy and the confidentiality of their PI/PHI are comprehensive, aligned and complementary.

18. The Agency shall comply with its policies and practices that protect individuals' privacy and the confidentiality of PI/PHI.

19. The Agency may consult with external and internal stakeholders in the development of its policies and practices that protect privacy and the confidentiality of PI/PHI.

Privacy Training and Awareness

20. The CPO shall provide a foundational privacy training program suitable for all personnel. The CPO shall review and update the program at least annually to address any substantive changes to eHealth Ontario's privacy requirements and any other relevant matters.

21. The CPO, supported by the Privacy Office, shall develop and provide role-based privacy training for personnel commensurate with their responsibilities and whether or not personnel may have

access to PI/PHI.

22. Personnel⁴ shall:

- sign the Acknowledgement and Agreement of the Privacy and Security Standard of Conduct prior to commencing their work with the Agency;
- complete foundational privacy training within thirty (30) days of beginning work at eHealth Ontario, and annually thereafter; and
- undertake role-based privacy training as directed by eHealth Ontario managers.

23. The Vice President, Human Resources and the Senior Director, Strategic Sourcing and Vendor Management shall:

- implement procedures to enable personnel to sign the Acknowledgement and Agreement of the Privacy and Security Standard of Conduct and complete privacy training in a timely manner; and
- provide regular compliance reports to eHealth Ontario managers and to the CPO.

24. eHealth Ontario managers shall ensure that personnel reporting to them meet their privacy training requirements.

Working with Third Party Providers

25. eHealth Ontario shall enter into signed, written agreements with third party providers that include appropriate privacy requirements prior to the third parties providing services or goods to the Agency.

26. With guidance from the CPO, the Senior Director, Strategic Sourcing and Vendor Management shall maintain standard content about privacy for procurement templates (e.g. privacy requirements, assessment and scoring criteria) and for agreements with third party providers. The CPO and Senior Director shall periodically review and update the standard content.

27. The Agency shall modify the standard content to reflect the nature of the services or goods that a third party provider will deliver, any specific privacy requirements arising and the associated privacy-related risks.

⁴ Personnel here means Agency employees and temporary staff working on eHealth Ontario premises with access to PI/PHI who are granted access to the eHealth Ontario network..

Protecting PI/PHI

28. eHealth Ontario shall protect PI/PHI with technical, administrative, and physical safeguards that:

- are appropriate to the information's sensitivity, the format in which it is held, and the related privacy risks; and
- secure the PI/PHI against: theft, loss, unauthorized collection, use or disclosure and unauthorized copying, modification or disposal.

29. Personnel shall not access PI/PHI unless:

- access is necessary in order to perform their roles;
- they have been authorized to do so by an eHealth manager with the requisite authority;
- they have signed the Acknowledgement and Agreement of the Privacy and Security Standard of Conduct and completed applicable privacy training;
- they have formally agreed to comply with any additional privacy-related requirements and restrictions established by eHealth Ontario; and
- they are in compliance with all applicable Agency policies.

Openness

30. The Agency shall publish its privacy policies and practices on its website and make copies of them available through the Privacy Office. For the benefit of clarity, the Agency shall not publish or make available policies or practices if doing so could compromise the security of PI/PHI or would reveal a trade secret or confidential scientific, technical, commercial or labour relations information.

31. eHealth Ontario shall publish the CPO's name, title and contact information on its website and advise individuals of this information on request.

32. eHealth Ontario shall publish summaries of the results of privacy assessments carried out on eHealth Ontario's services.

Monitoring Compliance and Performance

33. eHealth Ontario shall conduct privacy compliance reviews on a basis and schedule set by the CPO. A report shall be provided not less than annually to the Audit Committee of the Agency's Board of Directors.

34. eHealth Ontario shall maintain privacy-related performance metrics. The CPO shall regularly report on the metrics to the eHealth Ontario Executive Committee and, as required, to the eHealth Ontario Board of Directors.

Complaints and Inquiries

35. The Director, Privacy shall manage and respond to complaints, questions and feedback about the Agency's privacy practices.

36. The Agency shall review, investigate and document every complaint received and shall monitor for any trends arising.

37. If the sender provides contact information, the Agency shall:

- acknowledge the complaint, question or feedback within five (5) business days of receipt and provide information about any relevant internal and external complaint mechanisms;
- respond to the sender's question, feedback or complaint within thirty (30) business days of receipt; and
- notify the sender of its expected timeframe for responding if it anticipates a delay arising.

38. The Agency shall take appropriate measures to respond to complaints and feedback, which may include changing its policies and practices.

39. The Agency shall provide a means for personnel to share privacy-related concerns in confidence and shall ensure that reporting personnel suffer no reprisals.

Consequences

40. eHealth Ontario shall take appropriate remedial action to address non-compliance with its privacy requirements.

41. The consequences of non-compliance or for failing to take appropriate remedial action shall be consistent with the Agency's disciplinary and procurement policies and procedures and may include invoking measures up to and including dismissal or termination of contract.

5 Responsibilities:

5.1 Board of Directors

- Approves this Policy.

5.2 President and CEO

- Recommends this Policy for approval.

5.3 Chief Privacy Officer

- Maintains this Policy;
- Implements and enforces this Policy; and
- Is the ultimate authority for interpreting this Policy.

5.4 Privacy Office

- Provides advice, support and direction on interpreting and applying this Policy

5.5 eHealth Ontario Personnel

- Must comply with this Policy, to the extent that it applies to their activities

6 Glossary

Term	Definition
Accountability	The obligation to answer for results and the manner in which responsibilities are discharged. Accountability cannot be delegated.
Data Protection	Legislation such as Ontario's PHIPA and FIPPA protect individuals' privacy in respect of their PHI and PI. The laws establish rules about the collection, use and disclosure of PHI/PI and rights for individuals, e.g. the right to access their PHI/PI. Protecting individuals' privacy in this way is also known as 'informational privacy' or 'data protection'. More broadly, privacy is recognized as a human right and the right to privacy is generally accepted as a precursor to sustaining freedom and democracy. For example, in R v O'Connor, Justice L'Heureux-Dube found that 'respect for individual privacy is an essential component of what it

Term	Definition
	<p>means to be “free” and that the “essence of privacy... is that, once invaded, it can seldom be regained.”⁵</p> <p>The Agency’s Privacy and Data Protection Policy reflects the fact that protecting privacy involves, but may not be limited to protecting PI/PHI.</p>
eHealth Ontario managers	The President and CEO, Senior Vice Presidents, Vice Presidents, Senior Directors, Directors, Managers, Supervisors, program leads, project managers and personnel who carry out managerial duties
eHealth Services	One or more services to promote the delivery of health care services in Ontario that use electronic systems and processes, information technology and communication technology to facilitate electronic availability and exchange of information related to health matters, including personal information and personal health information, by and among patients, health care providers and other permitted users. (Enabling Regulation, s.1)
Enabling Regulation	Ontario Regulation 43/02, as amended from time to time, made pursuant to s.5 of the <i>Development Corporations Act</i> R.S.O. 1990, c. D. 10.
Governance	The processes and structures through which power and authority are exercised, including the decision-making processes.
Health Information Custodian	Has the same meaning as defined in section 3 of <i>Personal Health Information Protection Act, 2004</i> (PHIPA). Examples include: physicians, hospitals, pharmacies, laboratories, community care access centres and the Ministry of Health and Long-Term Care but not eHealth Ontario.
Personal Information	Has the meaning set out in section 2 of the <i>Freedom of Information and Protection of Privacy Act</i> (FIPPA) as: recorded information about an identifiable individual, including, (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual, (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved, (c) any identifying number, symbol or other particular assigned to the individual, (d) the address, telephone number, fingerprints or blood type of the individual, (e) the personal opinions or views of the individual except where they relate to another individual, (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence, (g) the views or opinions of another individual about the individual, and (h) the individual’s name where it appears with other Personal Information relating to the individual or where the disclosure of the name would reveal other Personal Information about the individual.
Personal Health Information	Has the meaning set out in section 4 of the <i>Personal Health Information Protection Act, 2004</i> (PHIPA), and generally means identifying information about an individual in oral or recorded form pertaining to that person’s health or health services provided to the individual.
Personnel	eHealth Ontario employees and temporary staff (contractors, temp agency staff, co-op students)

⁵ R v O’Connor [1995] 4 S.C.R. 411 at paragraph 119

Term	Definition
	and seconded individuals.) Contractors are individuals procured through a company for a specified period of greater than 3 months to fill a permanent full time position temporarily and on a day- to-day basis are managed directly by eHealth Ontario management.
Privacy default	A solution design that automatically protects privacy (i.e. the individual whose PI/PHI is involved needs to take no action to protect his/her privacy.)
Responsibility	The obligation to assume a role or take specific action(s). Responsibility may be delegated or conferred by mutual agreement, depending on the relationship.
Risk	The chance of something happening that will affect the achievement of objectives. Risk can represent an opportunity or threat to the achievement of objectives.
Risk assessment	The identification and analysis of relevant risks to the achievement of assigned objectives. Risk assessment is a prerequisite for determining how risks should be managed.
Risk management	The active process of systematically identifying risks, assessing exposures, and developing appropriate action plans so that risks are managed in a way that will enable a recipient to meet its business objectives.
Third party service providers	Entities that eHealth Ontario engages to support the delivery of its operations and services. They provide goods or services.

7 Subordinate Policies

The subordinate policies of the eHealth Ontario Privacy and Data Protection Policy as of October 13, 2011 are:

- eHealth Ontario Personal Health Information Privacy Policy
- eHealth Ontario Personal Information Privacy Policy
- eHealth Ontario Privacy Impact Assessment Policy
- eHealth Ontario Privacy Incident Management Policy
- eHealth Ontario Privacy Complaints and Inquiries Procedure
- eHealth Ontario Privacy Policy on the Responsibilities of Third Party Service Providers
- eHealth Ontario Information Security Policy
- eHealth Ontario Enterprise Security and Privacy Incident Management Program

8 Contact Information

For further information about this Policy, kindly contact:

Privacy Office
eHealth Ontario
P.O. Box 148
777 Bay Street, Suite 701
Toronto, ON
M5G 2C8

Fax: (416) 586-6598

Email: privacy@ehealthontario.on.ca

Telephone: (416) 946-4767

9 Interpretation

Policy requirements preceded by:

- 'shall' are compulsory actions;
- 'may' are options; and
- 'should' are recommended actions

If there is a discrepancy between this Policy and *FIPPA* or *PHIPA*, the regulations made under those Acts, or with the Agency's Regulation, the legislation or regulation takes precedence.

If there is a discrepancy between this Policy and any subordinate eHealth Ontario privacy and data protection policy, this Policy takes precedence.